$$(r,s,t) \leftarrow sign(x,m)$$

(1) Choose $a,b \in_R ZZ_q$ such that $a + bm \neq -1 \,(mod\ q)$

(2) $r \leftarrow m^a g^a \bmod p$

if $r, r - mx$ *or* $(a + bm)r + \mathrm{mx} = 0 \bmod \mathrm{q}$, then *repeat* from step (1).

(3) $(s,t) \leftarrow (ar\dfrac{mx - r}{(a + bm)r + mx}, m\dfrac{r - mx}{a + bm)r + mx})$

Fig. 1. Producing a signature

$$(m',(r',s',t')) \leftarrow trans(y,m,(r,s,t),\omega)$$

	Bob		Verifier
(1)	Choose $\alpha \in_R ZZ_q$		Choose $d \in_R ZZ_q^*$
(2)	$m' \leftarrow m^{\omega} \bmod p$		
(3)	$(\beta,\gamma) \leftarrow (\dfrac{rt}{m+t'}, \dfrac{ms - \omega(r+s)m'}{\omega(m+t)m'} - \dfrac{\alpha}{\omega m'})$		
	$r^* \leftarrow m^{\alpha} r^{\beta} g^{\gamma} \bmod p$	$\xrightarrow{m',r^*}$	
(4)		$\xleftarrow{d}$	
(5)	$r' \leftarrow (r^* y)^d g^{-\frac{1}{m'}} \bmod p$		$r' \leftarrow (r^* y)^d g^{-\frac{1}{m'}} \bmod p$
	if $dr' = 0\,(mod\ q)$ *then repeat from step* (1).		
(6)	$(a,b) \leftarrow (\alpha d, \beta d)$		
(7)	$(s',t') \leftarrow (\dfrac{art\text{ - }bms}{wrt} r' \bmod q, -m')$	$\xrightarrow{s',t'}$	*accept if* $verify(y,m',(r',s',t'))$

Fig. 2. Transforming a signature